Secure Web Fingerprint Transmission (SWFT) System
Public Key Infrastructure (PKI) Frequently Asked Questions (FAQs)

This document is current as of 28 Mar 14. The following set of responses to FAQs is provided in order to answer common questions regarding the Public Key Enablement of SWFT.

Table of Contents

1. **Will I have to get a new Smart Card or USB token to use SWFT aside from what I already use to access JPAS?**

   ANSWER: If your token works for JPAS, it will also work for SWFT.

2. **What will I need to log into SWFT?**

   ANSWER: Users will need three items to access SWFT with a Smart Card or USB token. These three items are:

   1. An active SWFT account. If you do not have one, refer to Question 3.
   2. An approved, active PKI Certificate on either a Smart Card or USB token (both are considered hardware). Refer to Questions 12 and 13.
   3. Hardware and software needed to read the PKI Certificate on the Smart Card or USB token. See Questions 16-19.
      - SWFT users with Smart Cards will need a Smart Card reader (hardware) and middleware (software) that can read the PKI certificate.
      - SWFT users with USB Tokens will only require middleware that can read the PKI certificate.

3. **How do I get a SWFT account?**

   ANSWER: The process and requirements for obtaining a SWFT account remains unchanged by PK-enabled log on. Visit the SWFT Home Page of the Personnel Security/Assurance (PSA) website (https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT) and refer to the Access Request Section on the left side of the SWFT Home page.

4. **Will SWFT accounts be handled differently (e.g., processing the PSSAR, unlocking of accounts, account management, etc.) now that SWFT requires the use of Smart Card or USB tokens?**

   ANSWER: SWFT did not change how accounts are obtained and managed. SWFT only changed the login procedure.

   If you enter your PIN incorrectly three times, you will likely lock the Smart Card or USB token. In such event, you will have to contact the PK token issuer. The DMDC Contact Center will be unable to provide assistance.

5. **Is a user ID and password required prior to logging in with a CAC or PKI certificate?**

   ANSWER: Yes, you must have an active user ID and password prior to accessing SWFT, as these are utilized on the self-registration page, where your SWFT account and PKI credential are correlated. You will only be required to input your user ID and password when registering a new certificate.

6. **Is there a difference in the login procedures for CAC users and non-CAC users like in JPAS?**

   ANSWER: No, CAC users and non-CAC users must both register their credentials in SWFT. PKI credentials are registered in SWFT using your username and password during your first PK-enabled logon. You will only register your PKI credential one time. Refer to Question 7 for additional information about re-registering a replacement credential in the event that your credential expires, is lost, or is stolen.

7. My Smart Card is going to expire soon, will I still be able to access SWFT once I receive a new credential?

ANSWER: If you are using a CAC, you will be able to log into SWFT with your new CAC without re-registering it.

If you use another type of approved PK token, then you will need to register your new credential. You can create a temporary password by yourself for your existing SWFT user account up to 72 hours before your old certificate expires, and then register your new certificate with that username and password. This process is explained in detail in the Users Guide, which can be accessed through the Help feature in the application.

8. Must I leave my CAC/PIV card inserted into my computer while I'm logged into SWFT?

ANSWER: The CAC/PIV card is only needed for authentication purposes, in order to prove that you are who you say you are, and also during random reauthentications during your session.

You should consult with your local IT department to determine if removing your CAC/PIV card will automatically lock your operating system and determine if your company or agency has a policy on the topic.

9. What is a Smart Card?

ANSWER: A Smart Card is a pocket-sized plastic card with an embedded integrated circuit chip. Smart Cards can be used to provide identification, authentication, data storage, and application processing. Smart Cards also store digital certificates along with other relevant identification data. The Common Access Card (CAC), Personal Identity Verification (PIV) card, and External Certification Authority (ECA) card are all examples of DOD-approved identity Smart Cards. While there are many applications for Smart Cards, we will use them only for authenticating the identity of the SWFT user.

10. What is a CAC and who qualifies for one?

ANSWER: The CAC, or Common Access Card, is a DoD Smart Card issued as the standard identification card for active-duty military personnel, reserve personnel, civilian employees, other non-DoD Government employees, state employees of the National Guard, and eligible contractor personnel. It allows holders to gain physical access to DoD facilities, and logical access to DoD computer systems and networks.

Only part of DoD Industry personnel are eligible for a CAC. DoD contractors who are under a DoD contract, *and* are sponsored by a DoD Service or Agency, may be eligible for a CAC if their Government sponsor deems it necessary and they fulfill one of the three following requirements (DoD Manual (DODM) 1000.13):

1. The user must work on site at a military or Government installation.
2. The user is a DoD contractor that works on Government Furnished Equipment.
3. The user has a contractual requirement for access to a Government facility or network.

To find out more information:

1. On the CAC, you can visit http://www.cac.mil/.

2. On the DODM 1000.13, Volume 1 http://www.dtic.mil/whs/directives/corres/pdf/100013_vol1.pdf.

11. What if I don't qualify for a CAC?

ANSWER: If you do not qualify for a CAC, there are other DoD approved Identity Credentials with PKI certificates (e.g. PIV cards, ECA PKI cards, or other DoD approved PKI cards) that are acceptable by the DoD, and can be used for accessing SWFT. See Question 12.

12. What other types of Identity Credentials contain DoD approved PKI certificates?

ANSWER: The following Identity Credentials contain DoD approved PKI certificates:

1. *PIV Cards*: PIV Cards are issued to many US Federal employees and contractors under HSPD-12 (as well as Federal Information Processing Standard (FIPS) 201[1]). Each Federal Agency is responsible for issuing PIV cards to qualifying employees and contractors.[2] Please use your internal procedures such as contacting your Security, Information Technology (IT), or Human Resource office to get additional information on determining qualifications for a PIV from your Federal Agency. Your Agency will explain the process for obtaining a PIV card as it varies from Agency to Agency. If you require access to Government facilities or property to complete the work that you are contracted to perform, it is likely that you will be issued a PIV by the Government.
2. *ECA Credentials*: This is designed to provide contractors a venue to procure DoD approved certificates. Only PKI certificates that obtained DoD approval for use in DoD systems can also be used for SWFT access. These need to be at a Medium Token Assurance or Medium Hardware Assurance certificate level – Do not assume a corporate Smart Card qualifies. For more information, please visit the following web site:
   - DISA's ECA PKI at http://iase.disa.mil/pki/eca/.
3. *PIV Interoperable Credentials*: Non-Federally issued PKI certificates that received DoD approval for use on DoD systems are also authorized for SWFT access. For more information, please visit the following web site:
   - A Complete list of DoD approved external PKI providers is available at: http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html http://iase.disa.mil/pki-pke/interoperability/index.html

13. How do I get a PKI certificate if my Agency does not issue PIVs and I don't qualify for a CAC?

ANSWER: If you do not qualify for either a CAC or a PIV, coordinate with your company to obtain a FIPS 140-2 compliant **Medium Token Assurance Certificate on a USB Token** or a **Medium Hardware Assurance Certificate on a Smart Card** from one of the three currently approved DoD ECA vendors listed below or go to http://iase.disa.mil/pki/eca/ for more information.

---

[1] FIPS 201-1 "Personal Identity Verification of Federal Employees and Contractors," http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[2] Homeland Security Presidential Directive-12 (HSPD-12) stipulates that personnel requiring regular access for more than 120-days to a Federally-controlled information system or facility shall be issued a PIV Card.

IdenTrust, Inc.
Web Site: http://www.identrust.com/certificates/eca/index.html
Email: ECAsales@IdenTrust.com
Phone: 866.299.3335

Operational Research Consultants, Inc.
Web Site: http://www.eca.orc.com/
Email: ecahelp@orc.com
Phone: 800.816.5548

VeriSign, Inc., (Now Symantec, also provides an NFI services in addition to ECA)
Web Site: http://www.symantec.com/page.jsp?id=eca-certificates
Email: eca-support@verisign.com or eca-support@symantec.com
Phone: 866-202-5570

Alternately, multiple Non-Federal Issuers (NFI) have been approved for PKI/cryptographic usage within the DoD. They include all of the listed Category II providers at the following website: http://iase.disa.mil/pki-pke/interoperability/index.html

You can also find the publicly available DoD approved PKI vendors at the following site: https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=DoD+approved+PKI+Vendors.pdf

14. Are there any questions I need to ask the ECA vendor when I first call them?

ANSWER: Be sure to ask the following questions:
"Do you provide the PKI Medium Token or Medium Hardware certificates on FIPS 140 compliant devices?"

- ECA certificates must be at a Medium Token or Medium Hardware level and must be generated directly on FIPS 140 compliant devices.

"What are the timelines associated with your credential issuance?"

- The processes and timelines for each issuer are different. It is advised that you ask what the timeline to be issued a credential will be before agreeing to purchase so that you will be able to plan accordingly.

"What is your PIN/Password reset policy?"

- Some ECA issuers and issuers of other DoD approved PKI credentials do not conduct PIN/Password resets and require the purchase of new credentials. Asking about the vendor's policy for PIN/Password resets will help you to make an informed decision.

15. What do I do when the PKI vendor offers me a thumb drive instead of a Smart Card?

ANSWER: FIPS 140 compliant Medium Token Assurance USB Tokens are acceptable. Please contact your IT department to ensure all internal policies and procedures of your organization will be followed prior to purchasing any PKI related equipment.

16. What hardware will I need to logon to SWFT using a Smart Card?

ANSWER: *A Smart Card Reader* – Please refer to the FIPS 201 Approved Products List for Smart Card readers, referred to as "Transparent Readers," located at: http://fips201ep.cio.gov/apl.php. Scroll down the list to find approved "Transparent Readers".

17. What hardware will I need to logon to SWFT using a USB Token?

ANSWER: Typically, every recently purchased computer has a USB interface. Installing additional middleware software may be needed.

18. What software will I need to logon to SWFT using a Smart Card or USB Token?

ANSWER:

1. *Step One*: Please check with your Department, Agency, or company's IT staff. Many Departments, Agencies, and companies already have existing Smart Card middleware installed within their infrastructure. Otherwise, please go to Step Two.

2. *Step Two*: Refer to the FIPS 201 Approved Products List for assistance with identifying which Smart Card middleware is authorized for use with the approved PKIs. There are over a dozen authorized PIV Middleware products. Many approved PKI vendors have the option to bundle deals to include the necessary hardware and software.

   Please refer to the FIPS 201 Approved Products List for the Smart Card middleware, referred to as 'PIV Middleware' located at: http://fips201ep.cio.gov/apl.php. Simply click Category on the top row to alphabetically sort the list of products. Then scroll down to the list of "PIV Middleware" for the complete listing.

   The PKI providers may direct their consumers to specific Smart Card readers and/or middleware that work best with their product.

19. If I have a CAC or PIV, do I need to purchase an additional certificate?

ANSWER: If you have an active CAC or PIV, then you will not need to purchase any additional certificates. It is possible, though, that you may still need to purchase additional hardware or software so that the CAC can be read from your computer. See questions 16 and 18.

20. What should an FSO do if his or her organization does not meet all the pre-requisites for Smart Card login during the Phase 1 period?

ANSWER: Until you obtain a DoD approved Smart Card or USB token, you will not be able to access SWFT when Phase 1 (transition period) is over. You may have to use the services of another DoD contractor or one of the 3rd party service providers to submit electronic fingerprints on your behalf. Refer to SWFT documentation published on the PSA website (https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=SWFT) for details.

21. If I already use a "soft" token from an approved PKI vendor, will I be able to login to SWFT?

ANSWER: No, you will not be able to login to SWFT with a "soft" token. PKI certificates must be loaded onto a FIPS 140-2 compliant device. Refer to Questions 12 and 13 for additional information on security requirements and approved vendors.

22. What if I forgot the PIN or Password for my credential?

ANSWER: This depends on the specific type of credential that you are using:

1. *DoD CACs*: You have 3 attempts to enter a correct PIN. If you fail the 3rd attempt, then your credential will be locked, and you will need to visit a DEERS/RAPIDS station to have it unlocked.
2. *Federal PIV Cards*: A procedure to similar to what is required to unlock a CAC will be required to unlock your PIV Card.
3. *ECA Credentials and other DoD approved PKI credentials*: This process may vary from issuer to issuer.
   - Note: Some issuers do not conduct PIN/Password resets and will require the purchase of a separate credential. Please be forewarned and ask what the vendor's reset policy is prior to purchasing a PKI credential.

23. What do I do if I can't login using my CAC?

ANSWER: If you receive an "X509 error," please close all browser windows, even those not associated with SWFT. It is likely that your previous login attempt or session is still active in your Internet browsing history. After closing all of your browser windows, try accessing SWFT again.

In addition, a temporary work-around has been developed regarding this specific error message:

Select Tools > Internet Options > Content Tab > Select the "Clear SSL State" toggle button. After this, close the options windows and logon to SWFT as normal.

If this does not solve the problem, refer to Sections 3 and 4 of the JPAS PKI Technical Troubleshooting Guide. Lastly, if these steps do not resolve the issue, call the DMDC Contact Center at 1-800-467-5526 for technical assistance.

24. I was able to login to SWFT with a Smart Card or USB token previously. Why am I now unable to access SWFT?

ANSWER: There are two possible reasons.

1. If you recently changed your name so that the name on your Smart Card or USB Token no longer matches the name on your SWFT account, you will need to contact your Account Manager (or DMDC Contact Center, if you are an Account Manager) and have them correct your name on your account.

2. If you have not changed your name recently, check with your internal IT department to ensure that your web-proxy is allowing connectivity from all '*.dmdc.mil.' If you are still unable to access SWFT, call the DMDC Contact Center at 1-800-467-5526 for technical assistance.

25. What is PKI?

ANSWER: PKI, or Public Key Infrastructure, is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

PKI enables users of an unsecure public network, such as the Internet, to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained from a trusted authority. The PKI also provides a digital certificate that can identify an individual, organization, or directory services.

A public key infrastructure consists of:

1. A Certification Authority (CA) that issues and verifies the digital certificate. A certificate includes the public key or information about the public key of the user.
2. A Registration Authority (RA) that acts as the verifier for the CA before a digital certificate is issued to a requestor.
3. One or more directories where the certificates (with their public keys) are held.
4. A certificate management system.

26. What is FIPS 140-2?

ANSWER: FIPS, or Federal Information Processing Standard, 140-2 is a Government computer security standard for accrediting cryptographic modules. The National Institute of Standards and Technology (NIST) issued the FIPS 140 series to coordinate the requirements and standards for cryptography modules that include both hardware and software components.

27. What is FIPS 201?

ANSWER: FIPS 201 is a Government standard that specifies PIV requirements for Federal employees and contractors. In response to HSPD-12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD 12 approved by the Secretary of Commerce on February 25, 2005. The Smart Card Interagency Advisory Board has indicated that in order to comply with FIPS 201 PIV II, US Government agencies should use smart card technology. FIPS 201 can be found at this site: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

28. What is HSPD-12?

ANSWER: HSPD-12 is a presidential directive that mandates a federal standard for secure and reliable forms of identification. Though not an official DoD source, for more information you can also visit http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#0.

29. What is middleware?

ANSWER: Middleware is software that provides a link between separate software applications. Middleware may be compared to plumbing because it connects two applications and passes data between them. In our scenario, it allows the computer to communicate with the smart card reader. Because most smart card readers connect to computers via USB connectors, the middleware is typically automatically installed.